DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS

A Thesis

Submitted in the partial fulfillment of the requirement for the award of the Degree of

BACHELOR OF ENGINEERING

IN

INFORMATION TECHNOLOGY

BY

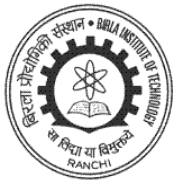
VAIBHAV MISHRA (BE/1365/2010)

ROHIT HARSHVARDHAN (BE/1361/2010)

UNDER GUIDANCE OF

DR. VIJAY KUMAR JHA

ASSOCIATE PROFESSOR



DEPT. OF INFORMATION TECHNOLOGY

BIRLA INSTITUTE OF TECHNOLOGY

MESRA-835215, RANCHI 2013

DECLARATION CERTIFICATE

This is to certify that the work presented in the thesis entitled "**Dynamic Routing with Security Considerations**"

in partial fulfillment of the requirement for the award of Degree of **Bachelor of Engineering in INFORMATION TECHNOLOGY** of Birla Institute of Technology, Mesra, Ranchi is an authentic work carried out under my supervision and guidance.

To the best of my knowledge, the content of this thesis does not form a basis for the award of any previous Degree to anyone else.

Date:

Dr. Vijay Kumar Jha
Dept. of IT
Birla Institute of Technology
Mesra, Ranchi-835215

CERTIFICATE OF APPROVAL

The foregoing thesis entitled "**DYNAMIC ROUTING WITH SECURITY CONSIDERATIONS**", is hereby approved as a creditable study of research topic and has been presented in satisfactory manner to warrant its acceptance as prerequisite to the degree for which it has been submitted.

It is understood that by this approval, the undersigned do not necessarily endorse any conclusion drawn or opinion expressed therein, but approve the thesis for the purpose for which it is submitted.

(Internal Examiner) **(External Examiner)**

(Chairman)

Head of the Department

ACKNOWLEDGEMENT

We owe our deepest gratitude to our guide **Dr. Vijay Kumar Jha**, who helped us throughout the project. He made sure that we learnt by practice, always motivating us to think a step further, work a little harder. Our interactions with him always resulted in newer ideas and proved beneficial towards our work. Without his constant presence and supervision our work would not have been successful.

We especially acknowledge the many useful discussions we had among ourselves that helped us understand some of the subtle technical problems in a better way.

Vaibhav Mishra (BE/1365/2010)

Rohit Harshvardhan (BE/1361/2010)

CONTENTS

ABSTRACT

Security has become one of the major issues for data communication over wired and wireless networks. To enhance the security of data transmission, existing system works on the cryptography based algorithms such as SSL, IPSec. Although IPSec and SSL accounts for great level of security, they introduce overheads. A mass of control messages exchanging also needed in order to adopt multiple path deliveries from source to destination.

Different from the past work on the designs of cryptography algorithms and system infrastructures, we will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of the proposed algorithm.

CHAPTER 1

PROBLEM STATEMENT

1.1 INTRODUCTION

In the past decades, various security-enhanced measures have been proposed to improve the security of data transmission over public networks. Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc. Among many well-known designs for cryptograph based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads especially on gateway/host performance and effective network bandwidth.

For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) is adopted for

encryption/decryption for IPSec. Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adapting of multiple paths between a source and a destination to increase the throughput of data transmission.

1.2 OBJECTIVE

The main objective is to propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages. The objective of this work is to explore a security enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks.

We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted packets.

The proposed algorithm should be easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) for wired networks and Destination-Sequenced Distance Vector (DSDV) protocol for wireless networks, over existing infrastructures. These protocols shall not increase the number of control messages

if the proposed algorithm is adopted. An analytic study will be presented for the proposed routing algorithm, and a series of simulation study will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

1.3 MOTIVATION

In Static Routing, the routes are entered manually. It is the best solution when we have small networks, and the networks do not change very often. When we say change we mean new host and networks are not frequently added are removed. While dynamic route are best suited when the network structure is very dynamic. Dynamic routes use network resources to learn where all host are, and the structure of the network. To enhance the dynamic routing with security considerations. We choose randomization of path deliveries with the help of the Dynamic Routing Protocol namely DSR (Dynamic Source Routing).

CHAPTER 2
THEORETICAL BACKGROUND

2.1 PRESENT SYSTEM

Present network on security enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the internet, including eavesdropping, spoofing, session hijacking, etc. Among many well-known designs for cryptography based systems, the IP Security and the Secure Socket Layer are popularly supported and implemented in many systems and platforms. Although IP Security and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads, especially on gateway or host performance and effective network bandwidth.

2.2 LITERATURE SURVEY

Some popular routing protocols related to the present system are:

1. Adaptive Routing
2. Multipath Routing
3. Zone Routing Protocol

2.2.1 ADAPTIVE ROUTING

Adaptive routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change. People using a transport system can display adaptive routing. For example, if a local railway station is closed, people can alight from a train at a different station and use another method, such as a bus, to reach their destination.

The term is commonly used in data networking to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. There are several protocols used to achieve this:

- RIP
- OSPF

Systems that do not implement adaptive routing are described as using static routing, where routes through a network are described by fixed paths (statically). A change, such as the loss of a node, or loss of a connection between nodes, is not compensated for. This means that anything that wishes to take an affected path will either have to wait for the failure to be repaired before restarting its journey, or

will have to fail to reach its destination and give up the journey.

2.2.2 MULTIPATH ROUTING

Current routing schemes typically focus on discovering a single "optimal" path for routing, according to some desired metric. Accordingly, traffic is always routed over a single path, which often results in substantial waste of network resources. Multipath Routing is an alternative approach that distributes the traffic among several "good paths instead of routing all traffic along a single "best" path.

Equal-cost multi-path (ECMP) is a routing technique for routing packets along multiple paths of equal cost. The forwarding engine identifies paths by next-hop. When forwarding a packet the router must decide which next-hop (path) to use.

2.2.3 ZONE ROUTING PROTOCOL

The Zone Routing Protocol (ZRP) was introduced in 1997 by Haas and Pearlman. It is either a proactive or reactive protocol. It is a hybrid routing protocol. It combines the advantages from proactive (for example AODV) and reactive routing (OLSR). It takes the advantage of pro-active discovery within a node's local neighborhood (Intrazone Routing Protocol (IARP)), and using a reactive protocol for communication between these neighborhoods (Interzone

Routing Protocol (IERP)). The Broadcast Resolution Protocol (BRP) is responsible for the forwarding of a route request.
ZRP divides its network in different zones. That's the nodes local neighborhood. Each node may be within multiple overlapping zones, and each zone may be of a different size. The size of a zone is not determined by geographical measurement. It is given by a radius of length, where the number of hops is the perimeter of the zone. Each node has its own zone.

2.3 RELATED WORKS

- Lou et al. proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries. The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed.
- Bohacek et al. proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by Lou et al. A set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, a mass of control messages is needed.
- Yang and Papavassiliou explored the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided

that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path searching approaches, the discovery of multiple paths involves a significant number of control signals over the Internet.

2.4 THREATS TO THE EXISTING SYSTEM

Aside from the threat of unauthorized users accessing your network and eavesdropping your internal network communications by connecting with your wireless LAN (WLAN), there are a variety of threats posed by insecure or improperly secured WLAN's. Here is a brief list with descriptions of some of the primary threats:

2.4.1 Rogue WLAN's

Whether your enterprise has an officially sanctioned wireless network or not, wireless routers are relatively inexpensive, and ambitious users may plug unauthorized equipment into the network. These rogue wireless networks may be insecure or improperly secured and pose a risk to the network at large.

2.4.2 Spoofing Internal Communications

An attack from outside of the network can usually be identified as such. If an attacker can connect with your WLAN, they can spoof communications that appear to come

from internal domains. Users are much more likely to trust and act on spoofed internal communications.

2.4.3 Theft of Network Resources

Even if an intruder does not attack your computers or compromise your data, they may connect to your WLAN and hijack your network bandwidth to surf the Web. They can leverage the higher bandwidth found on most enterprise networks to download music and video clips, using your precious network resources and impacting network performance for your legitimate users.

2.4.4 Network Eavesdropping or Network Sniffing

It is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information. The attack could be done using tools called network sniffers. These tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling.

CHAPTER 3

PROPOSED CHANGES TO THE EXISTING SYSTEM

3.1 INTRODUCTION

Each and every node in the network maintains a routing table which consists of the destination node, an estimated minimal cost to send a packet to the destination, the list of next nodes that can be chosen to reach the destination and the history record for packet deliveries. History of each packet delivery is considered in each case. The best aspect of this method is that there will no extra control messages. The data received will not show any evidence of security. The message to be sent is divided into number of packets. The source node will be distributing all the packets to different neighboring nodes from the list of next hops by considering the history.

The packet size has the most profound effect on the number of packets sent across the network. Here whatever the packet size and number of packets may be, no two consecutive packets will take the same path. Suppose, the complete data to be sent is divided into 12 packets and the possible next-hops are 10. 10 packets will be delivered to 10 different nodes and the remaining 2 will be sent through two different nodes among the available next hops. Care

has to be taken such that the path similarity is minimum. If the receiver can get a clarification that the packets are dynamically routed, our work is done. Each computer will have a unique address to communicate with each other. In order to enable the computers to communicate with each other on a network, the concept of the hostname is included.

The hostname was just a simple string of alphanumeric characters and a hyphen can also be used .Now it is a Fully Qualified Domain Name (FQDN) that absolutely and uniquely identifies every computer connected to the Network. Example of the hostname is: mypc-1477h123 An Internet Protocol address (IP address) is also a unique identifier for a computer or device on a TCP/IP network or a numerical label assigned to each device (e.g., computer, printer)participating in a computer network that uses the Internet Protocol for communication. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number among the four can be zero to 255. For example, 192.168.10.01 could be an IP address.

We propose that if the Host Name or the IP Address or any secure information that receiver also known (that information discuss before any data send) of the node

which is the first hop from the source is printed along with the data packet delivered through it, the receiver can ensure that the data packets are received in a secured way i.e. through different paths. Since IP Address is rather difficult to remember as they are not particularly descriptive, we can specify a computer by a Host Name rather than a number string. It is preferred to print Host Name along with the data packet. If this is implemented, the received data will be as follows, [host name 1] [data in the first packet] [host name 2] [data in the second packet]…… [host name n][data in the last packet]. By this an assurance that the data packets received are dynamically routed with minimum path similarity can be achieved.

In our proposed work we are also adopting vulnerability evaluation in both node as well as path. The vulnerable node is one in which is having more number of connections. The vulnerable path is one in which is having more nodes to reach the destination links between two delivery paths) of two consecutive transmitted packets. The node which is having more number of connections, that node is said to be vulnerable node. This evaluation will reduce the chance of getting hacked. The path which is having more number of nodes to cross, that path is said to be vulnerable path. These evaluations will be useful in future routing.

The proposed algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector Protocol in wireless networks, without introducing extra control messages.

3.2 METHODS APPLIED

3.2.1 BELLMAN FORD ALGORITHM

Bellman Ford algorithm computes single source shortest paths in a weighted digraph. For graphs with only non-negative edge weights, the faster Dijkstra's algorithm also gives solution to the problem. Thus, Bellman Ford is used for graphs with negative edge weights. Bellman Ford's basic structure is very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes all the edges, and does this |V|-1 time, where |V| is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles; the shortest path can only visit each node at most once. Unlike the greedy approach, which depends on some specific structural assumptions derive from positive weights; this straight forward approach extends to the general case.

3.2.2 ROUTING INFORMATION PROTOCOL

The Routing Information Protocol (RIP) is a distance vector routing protocol, which employs the hop count as a routing metric. The hold down time is 180 seconds. This protocol prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The maximum number of hops allowed for RIP is 15. The hop limit, however, also limits the size of networks that RIP can support. A hop count of 16 can be considered an infinite distance and used to deprecate inaccessible, inoperable, or otherwise undesirable routes in the selection process.

RIP implements the split horizon, route positioning and hold-down mechanisms to prevent in-correct routing information from being propagated. These are some of the stability features of RIP. It is also possible to use the Routing Information Protocol with Metric-based Topology Investigation (RMTI) algorithm to cope with the count-to-infinity problem. With its help, it is possible to detect every possible loop with a very small computation effort.

3.2.3 DESTINATION SEQUENCED DISTANCE VECTOR ROUTING

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad-hoc mobile networks based on the Bellman Ford algorithm. The main aim of the algorithm was to solve the routing loop problem where each entry in the routing table contains a sequence number, the

sequence numbers are generally even if a link is present or else an odd number is used. The number is generated by the destination, and the emitter has to send out the next update with this number. The routing information is distributed among the nodes by sending full dumps infrequently and smaller updates more frequently which are incremental. The procedure in section of the router is as follows. If a router receives a new information, them it uses the latest sequence number. If the sequence number is same as the one which is already present in the table, then the route with the better metric is used. And the left over entries which have not been updated for a while are called stale entries. Such entries and the routes using those nodes as next hops are deleted.

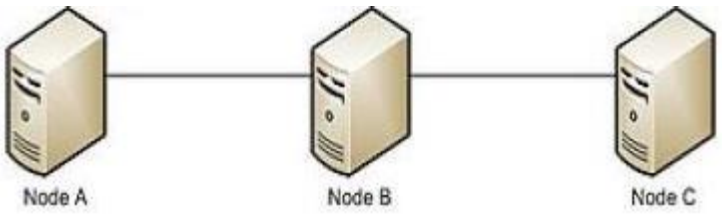


FIG-1

The Routing Table of Node-A in the network-

Destination	Next Hop	Number of Hops	Sequence Number
A	A	0	A46
B	B	1	B36
C	B	2	C28

Fig-2

3.3 ROUTING AND SECURITY CONSIDERATIONS

For security purpose, for delivering a data packet we use randomization process and maintain routing table based on bell-men ford algorithm.

3.3.1 RANDOMIZATION PROCESS

Consider the delivery of a packet with the destination t at a node Ni. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries. In this process, the previous next hop hs for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighbouring node in excluding hs as the next hop for the current packet transmission. The exclusion of hs for the next hop selection avoids transmit- ting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

3.3.2 ROUTING TABLE MAINTAINENCE

Let every node in the network be given a routing table and a link table. We assume that the link table of each node is constructed by an existing link discovery protocol, such as the Hello protocol. On the other hand, the construction and maintenance of routing tables are revised based on the well-known Bellman-Ford algorithm.

Bellman-Ford algorithm computes single source shortest paths in a weighted digraph. For graphs with only non-

negative edge weights, the faster Dijkstra's algorithm also gives solution to the problem. Thus, Bellman–Ford is used for graphs with negative edge weights. Bellman–Ford‘s basic structure is very similar to Dijkstra's algorithm, but instead of greedily selecting the minimum-weight node not yet processed to relax, it simply relaxes all the edges, and does this $|V| - 1$ times, where $|V|$ is the number of vertices in the graph. The repetitions allow minimum distances to accurately propagate throughout the graph, since, in the absence of negative cycles, the shortest path can only visit each node at most once. Unlike the greedy approach, which depends on some specific structural assumptions derived from positive weights, this straightforward approach extends to the general case.

FUTURE SCOPE OF WORK

Implementation of the Randomization process and Routing Table Maintenance. An analytic study on the proposed algorithm will be presented, and a series of simulation experiments will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

BIBLIOGRAPHY

1. T.H. Cormen, C.E. Leiserson and R.L. Rivest, Introduction to Algorithms.

2. D. Collins, Carrier Grade Voice over IP. McGraw-Hill, 2003.

3. G. Malvin, Routing Information Protocol (RIP) Version 2 Carrying additional Information, Request for comments (RFC 1723), Nov. 1994.

4. Secure Socket Layer (SSL), http://www.openssl.org/, 2008.

5. P. Erdo's and A. Renyi, "On Random Graphs", Publications.

6. W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery".